North Carolina
State Bureau of Investigation

Computer Forensics

Technical Procedure Manual

August 25, 2010

North Carolina State Bureau of Investigation
Digital Evidence Section
Computer Forensics Technical Procedure Manual

Any updates, modifications, additions, or deletions to this manual prepared after the date on the cover sheet must be approved by the SAC prior to their implementation.

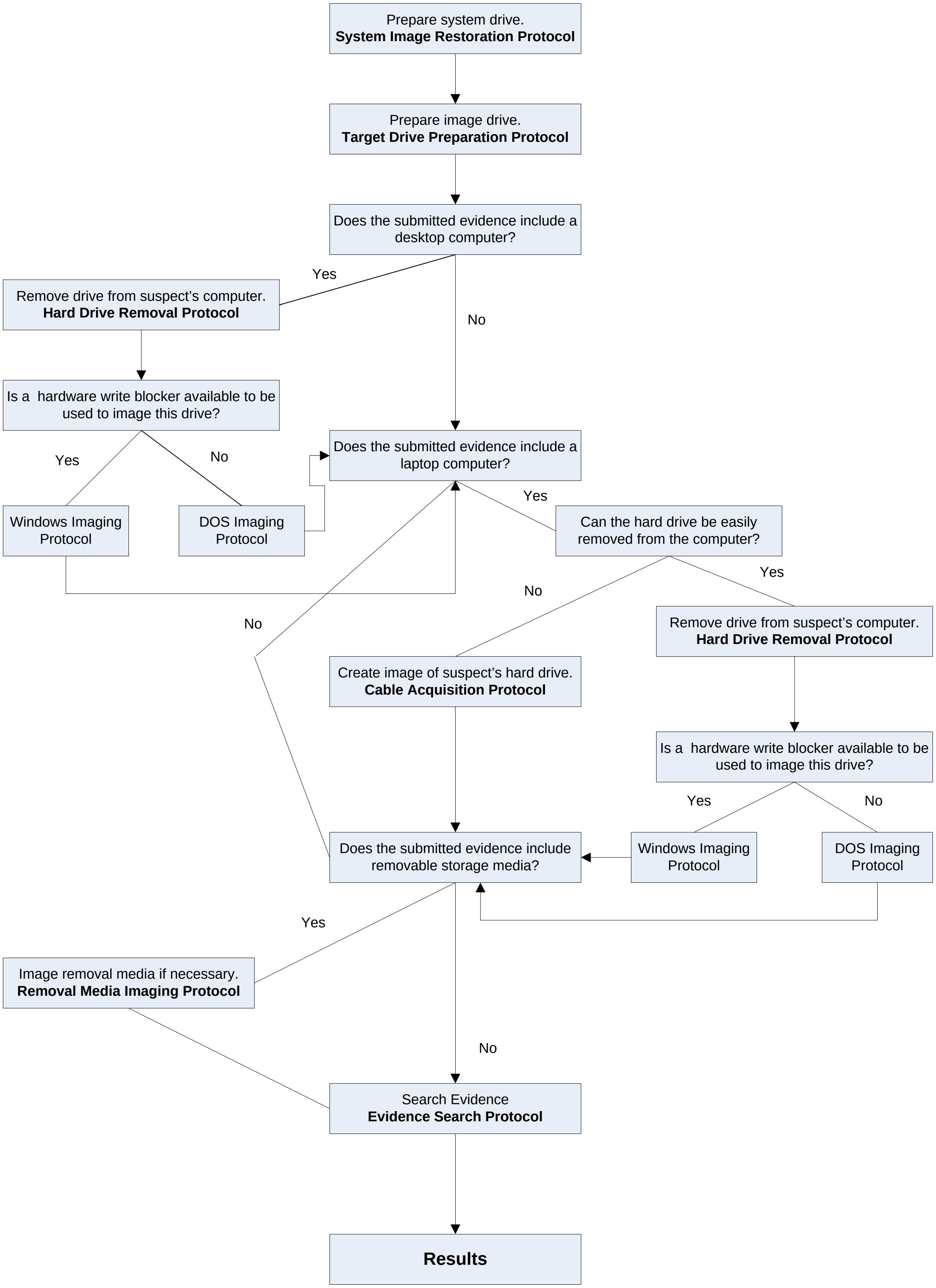
Upon revision, the prior version(s) of this document shall be archived.

The Assistant Director and Laboratory Quality Manager will review the section procedure manuals as a part of the annual quality audit. Documentation of these reviews will be stored on the Section’s shared document area.

Digitally signed by SAC Jonathan Dilday
DN: cn=SAC Jonathan Dilday, o=North Carolina SBI, ou=Digital Evidence Section, email=jdilday@ncdoj.gov, c=US
Date: 2010.08.25 15:48:36 -04'00'

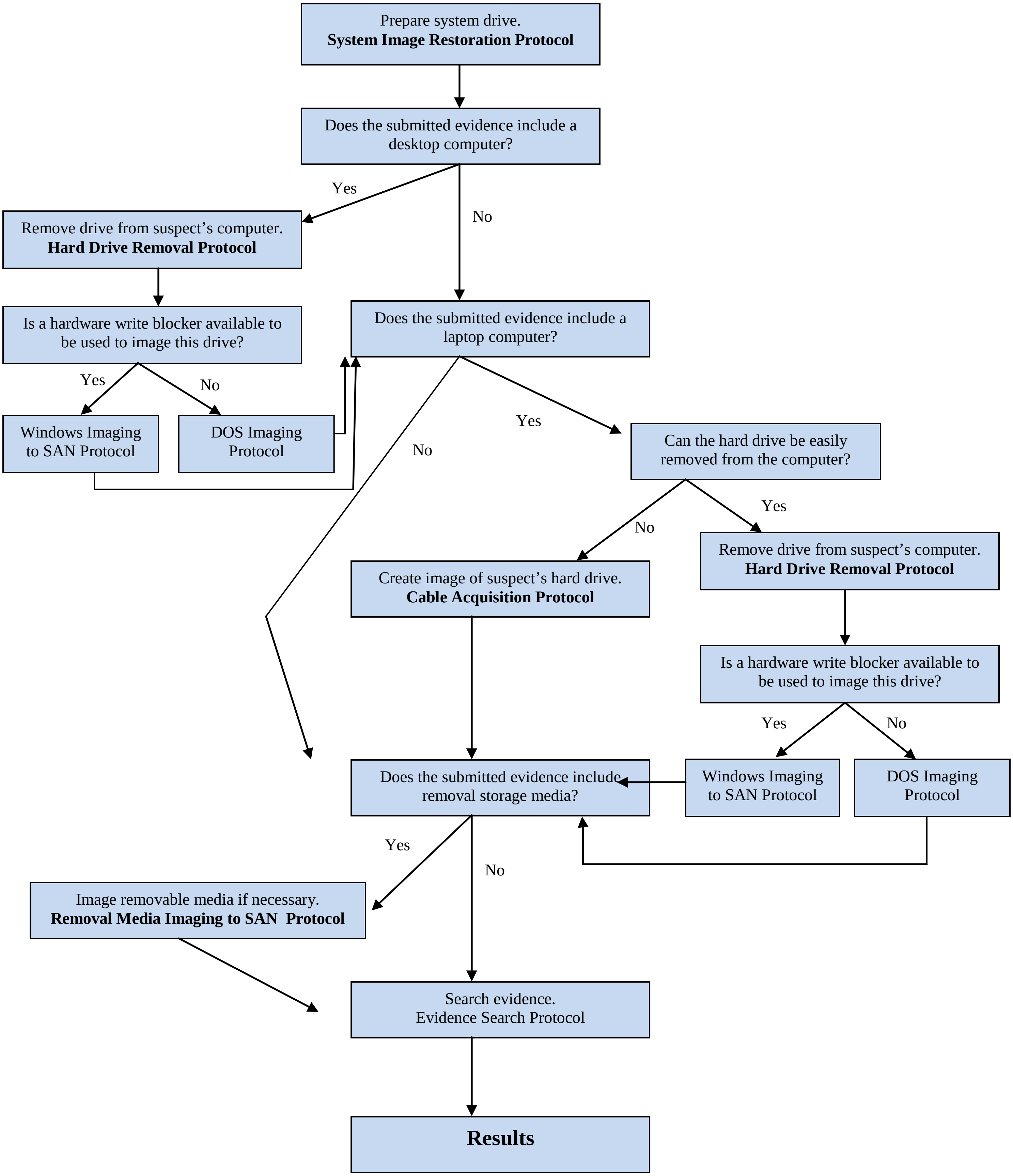
Table of Contents

General Flow Diagram for Forensic Computer Examination

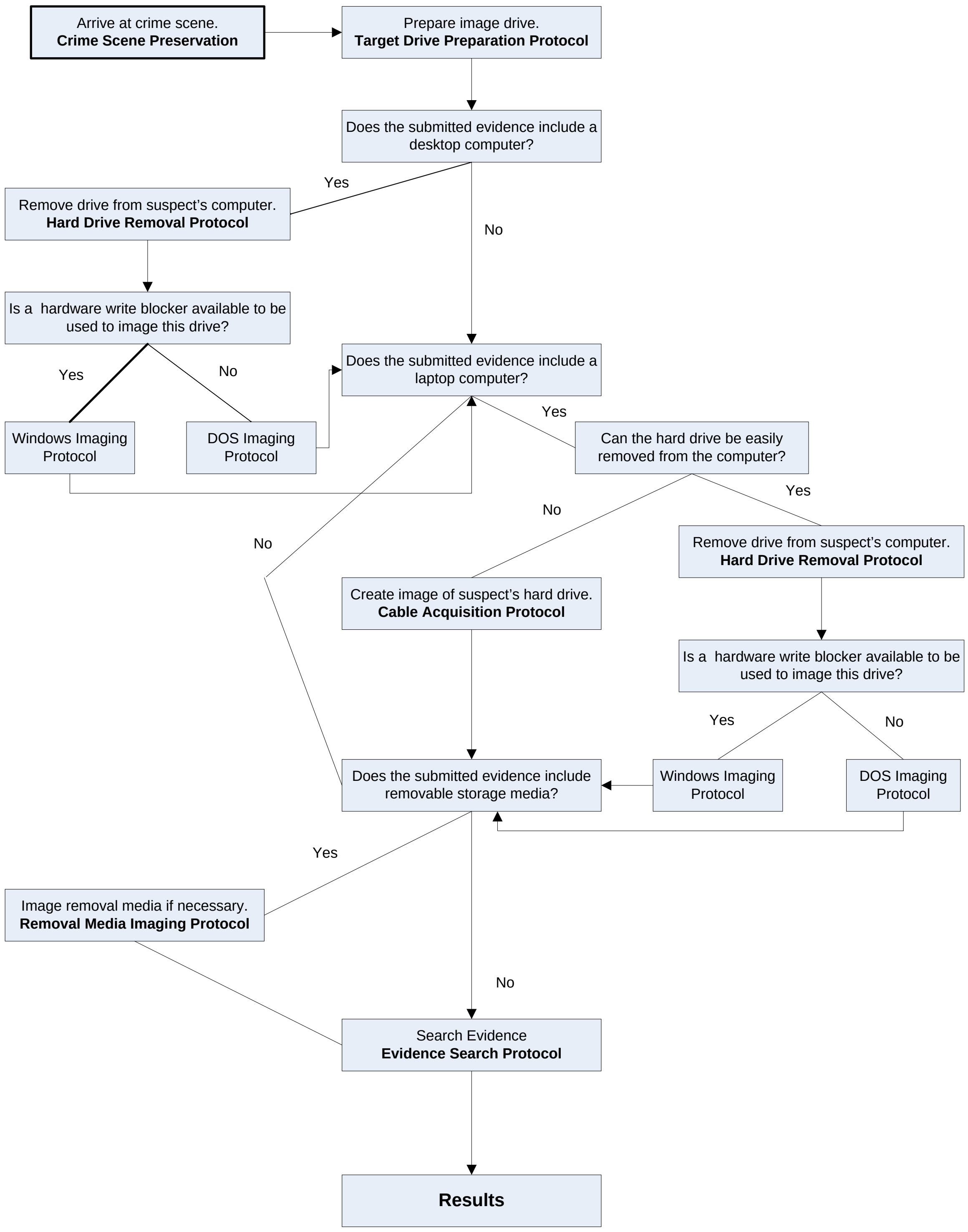


Prepare system drive.
System Image Restoration Protocol
Prepare image drive.
Target Drive Preparation Protocol
Does the submitted evidence include a desktop computer?
Yes
No
Remove drive from suspect's computer.
Hard Drive Removal Protocol
Is a hardware write blocker available to be used to image this drive?
Yes
No
Windows Imaging Protocol
DOS Imaging Protocol
Does the submitted evidence include a laptop computer?
Yes
Can the hard drive be easily removed from the computer?
No
Yes
No
Remove drive from suspect's computer.
Hard Drive Removal Protocol
Create image of suspect's hard drive.
Cable Acquisition Protocol
Is a hardware write blocker available to be used to image this drive?
Yes
No
Does the submitted evidence include removable storage media?
Windows Imaging Protocol
DOS Imaging Protocol
Yes
Image removal media if necessary.
Removal Media Imaging Protocol
No
Search Evidence
Evidence Search Protocol
Results

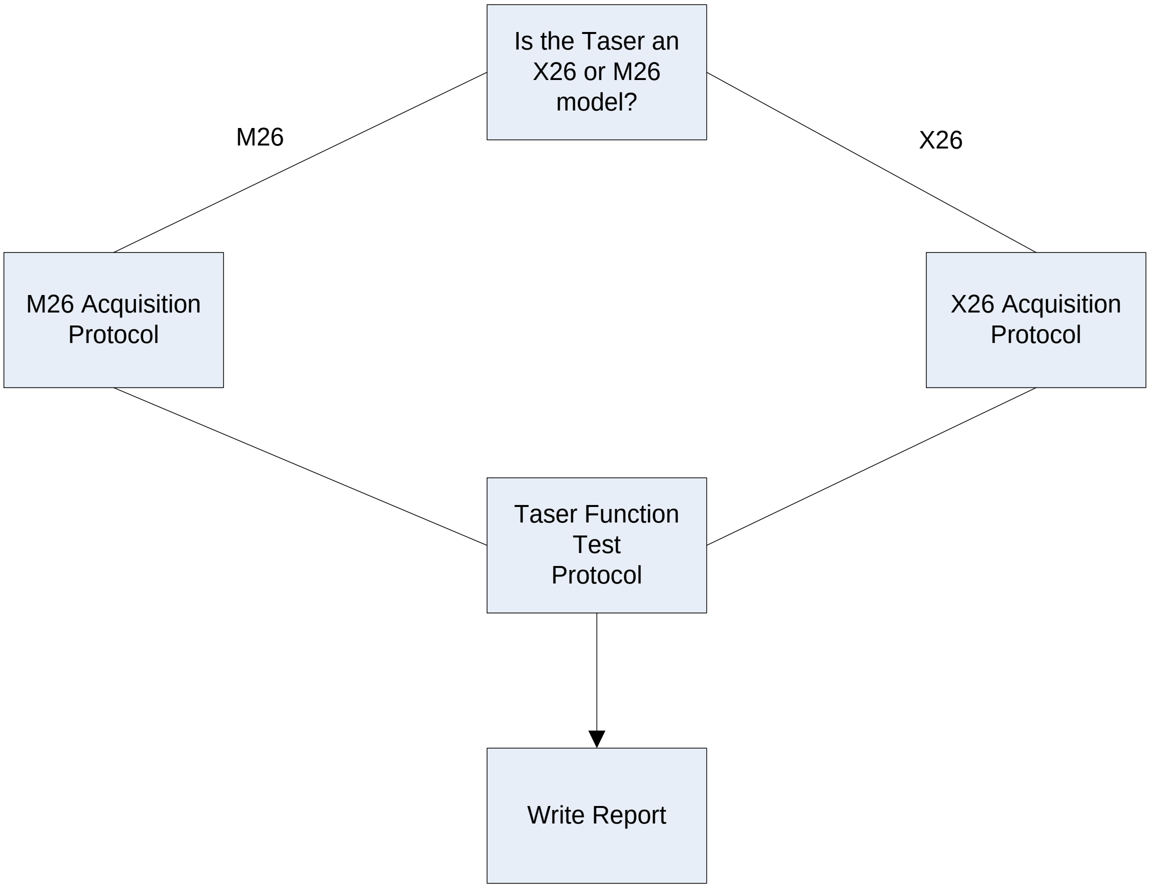
General Flow Diagram for Forensic Computer Examination with SAN


Prepare system drive.
System Image Restoration Protocol
Does the submitted evidence include a desktop computer?
Yes
No
Remove drive from suspect's computer.
Hard Drive Removal Protocol
Is a hardware write blocker available to be used to image this drive?
Yes
No
Windows Imaging to SAN Protocol
DOS Imaging Protocol
Does the submitted evidence include a laptop computer?
Yes
No
Can the hard drive be easily removed from the computer?
No
Yes
Create image of suspect's hard drive.
Cable Acquisition Protocol
Remove drive from suspect's computer.
Hard Drive Removal Protocol
Is a hardware write blocker available to be used to image this drive?
Yes
No
Windows Imaging to SAN Protocol
DOS Imaging Protocol
Does the submitted evidence include removal storage media?
Yes
No
Image removable media if necessary.
Removal Media Imaging to SAN Protocol
Search evidence.
Evidence Search Protocol
Results

General Flow Diagram for Forensic Computer Crime Scene Response


Arrive at crime scene.
Crime Scene Preservation
Prepare image drive.
Target Drive Preparation Protocol
Does the submitted evidence include a desktop computer?
Yes
No
Remove drive from suspect's computer.
Hard Drive Removal Protocol
Is a hardware write blocker available to be used to image this drive?
Yes
No
Windows Imaging Protocol
DOS Imaging Protocol
Does the submitted evidence include a laptop computer?
Yes
Can the hard drive be easily removed from the computer?
No
Yes
No
Remove drive from suspect's computer.
Hard Drive Removal Protocol
Create image of suspect's hard drive.
Cable Acquisition Protocol
Is a hardware write blocker available to be used to image this drive?
Yes
No
Does the submitted evidence include removable storage media?
Windows Imaging Protocol
DOS Imaging Protocol
Yes
Image removal media if necessary.
Removal Media Imaging Protocol
No
Search Evidence
Evidence Search Protocol
Results

Taser Examination



Title: Crime Scene / Field Response Evidence Preservation Protocol
Version: 1.2 (3/9/2010)

Introduction:

This procedure describes the steps to be taken by all personnel of the North Carolina State Bureau of Investigation when they are called upon to provide computer forensic assistance at crime scenes.

Purpose:

The purpose of this procedure is to secure digital evidence located at a crime scene and preserve its integrity for further forensic processing.

Equipment:

1. Camera
2. Clean 3 ½ inch floppy disk
3. Clean USB thumb drive, USB removable drive, or other blank media

Definitions:

Removable Media – digital storage media such as CDs, Zip disks, Jazz disks, floppy disks, and USB thumb drives which are not permanently installed in the computer.

Calibration:

None needed for this procedure.

Limitations:

1. Simply unplugging a suspect computer from a business network can cause data loss and damage the network.
2. Assistance should be sought from the system administrator in isolating the computer from the network, as long as the administrator is not a subject in the investigation.
3. If the system administrator is the subject, assistance should be sought from personnel knowledgeable in the network's operation.
4. Be sure all computers involved in the search are secured and that no one is allowed access to them. Important data can be quickly damaged or destroyed.
5. The computers at the scene should be searched to determine if any wireless networks exist. If one does exist, the computer of interest should be isolated from this network.
6. If at any point while securing the computer the analyst believes that evidence may be being destroyed, the power cord should be pulled from the back of the computer.
7. In shutting down a computer, the plug should be pulled from the back of the computer, not the wall outlet. If it is a laptop computer, the power cable and battery should be removed. If the computer is unplugged at the outlet, there may be a UPS backup on the system which will power the computer long enough to complete desired processes and do a soft shutdown of the computer.

8. When a cellular phone is present, great care should be taken to not allow the device to connect to its cellular network. Allowing the phone to receive a signal from the cellular network might result in a change in the data contained on the internal memory of the phone. For this reason, the phone should be turned off upon seizure.

Procedures:

1. Remove the subject from the computer and do not allow the subject access to it.
2. If the computer is networked, ensure that no one is allowed access to any of the computers until the computer of interest can be isolated from the network.
3. Document the condition of the computers with photographs and notes. This documentation should include any documents that are open and other information that may appear on the monitor such as the time given on the clock.
4. Save any open documents on the computer to a floppy disk. If the computer does not have a floppy drive or the file is too large, save it to a USB thumb drive, USB removable drive, or other blank media.
5. Shut down the computer by pulling the plug from the back of the computer. If it is a laptop computer, remove the power cable and battery.
6. Note the hardware connections to the computer with notes, pictures or both. Label the cords and the area that they are plugged into so the system can be reassembled at a later date if needed.
7. Search the scene for removable media.
8. Search the area around the computer for any passwords, account numbers, or other pertinent information which may have been written down.

References:

1. Seizing Electronic Evidence ; US Secret Service
2. Mechanics of Seizure ; S/A Jonathan L. Dilday, NCSBI

Notes:

1. It is important to document the condition of the computer before disassembling it. It is necessary to be able to put the computer back as it was when it was seized. For a laptop computer, seize its power cable and battery.
2. The crime scene should be searched thoroughly for removable media. In some cases, the evidence being sought will only reside on removable media.
3. If files on the computer are encrypted, finding the password written down near the computer may be the only way to access the information.

Title: System Image Restoration Protocol
Version: 1.1 (3/9/2010)

Introduction:
This procedure describes the steps to be taken by all personnel of the North Carolina State Bureau of Investigation in preparing system drives for use in forensic computer examinations.

Purpose:
The purpose of this procedure is to restore system drives used in forensic casework to a default state in order to ensure that no cross contamination occurs between cases.

Equipment:
1. Forensic Tower or Portable Forensic Workstation
2. Hard drive
3. Approved software for creating and restoring system images
4. Factory Restore Image on CD or DVD
5. Previously created system image (if available)

Definitions:
1. System drive – the drive that contains the operating system (OS).
2. System image – backup of drive that is used to prepare forensic tower for beginning new case.

Calibration:
The forensic towers used in casework must be verified each day that they are used to ensure that the computer hardware and software are functioning properly. The procedure for this verification process can be found in the Digital Evidence Unit Validation and Calibration Manual.

Limitations:
Failure to clean the information from a previously used hard drive can lead to the possibility of data from old cases contaminating a new case.

Procedures:
1. If a previously created system image is available, skip to step 5.
2. If no previously created system image is available, or updates to the default system image need to be made, use the original Restore Disk that came packaged with the Forensic tower or perform a fresh install of the operating system.
3. Install any software from the Approved Software for Forensic Computer Examinations to be included on System Image.
4. Use an approved backup utility to create an image of the system image and restore system drive.
5. Restore the system drive using the previously prepared system image.

References:

1. Digital Evidence Unit Validation and Calibration Manual

Notes:

None

Title: Target Drive Preparation Protocol
Version: 1.3 (3/9/2010)

Introduction:
This procedure describes the steps to be taken by all personnel of the North Carolina State Bureau of Investigation in preparing Target drives for use in forensic computer examinations.

Purpose:
The purpose of this procedure is to wipe all information from Target drives used in forensic casework in order to ensure that no cross contamination occurs between cases.

Equipment:
1. Forensic Tower or Portable Forensic Workstation
2. Hard drive
3. Approved software or hardware device for wiping data
4. F-disk or G-disk software programs as necessary

Definitions:
1. Target Drive – the drive that information from the evidence drive is being written to.
2. Wipe – permanently deleting all data from a drive by overwriting the data with a known value.

Calibration:
The forensic towers used in casework must be verified each day that they are used to ensure that the computer hardware and software are functioning properly. The procedure for this verification process can be found in the Digital Evidence Unit Validation and Calibration Manual.

Limitations:
Failure to wipe the information from a previously used hard drive can lead to the possibility of data from old cases contaminating a new case.

Procedures:
1. Select a Target drive that has sufficient storage capacity to hold the forensic image files and recovered files generated from the evidence hard drive.
2. Attach a label to the Target drive with the pertinent case information.
3. Use an approved wipe utility or approved hardware device such as the VOOM Hardcopy II to remove all information from the drive
4. Create a new primary partition on the Target drive.
5. Format the Target drive.
6. Enter a suitable name for the Target drive so that it will not be confused with other drives (forensic image, target, etc.).
7. Directories can be created on the drive in order to keep the evidence organized.

References:

1. EnCase Forensic User Manual
2. EnCase Intermediate Analysis and Reporting course guide
3. EnCase Advanced Computer Forensics course guide
4. Forensic Toolkit User Guide
5. Forensic Boot Camp Training Manual
6. Digital Evidence Unit Validation and Calibration Manual

Notes:

1. This procedure should be used for new hard drives as well as hard drives used in previous cases.
2. When responding to image a computer in the field, the Target drives should be prepared by this procedure prior to arriving at the scene. This will speed up the process of imaging the computer and will result in a shorter down time for the evidence computer.

Title: Hard Drive Removal Protocol
Version: 1.2 (3/9/2010)

Introduction:

This procedure describes the steps to be taken by all personnel of the North Carolina State Bureau of Investigation in removing hard drives from computers which are evidence in forensic computer examinations.

Purpose:

The purpose of this procedure is to remove the hard drives from computers submitted for examination while maintaining the integrity of the evidence.

Equipment:

1. Computer repair tool kit
2. Permanent markers
3. Camera

Definitions:

BIOS – Basic Input Output System. A number of machine code routines that are stored in ROM and available for execution at boot.

Calibration:

None needed for this procedure.

Limitations:

Precautions should be used to guard against electrostatic discharges which can damage or destroy the evidence hard drive.

Procedures:

1. Record the system information from the evidence computer.
2. If necessary, photograph the condition of the evidence computer prior to opening the case.
3. Open the case on the computer.
4. If necessary, photograph the internal contents of the evidence computer prior to removing the hard drive(s).
5. Mark the cords connecting the hard drive to the evidence computer.
6. Remove the hard drive(s) from the evidence computer.
7. Label the hard drive removed from the evidence computer to prevent evidence contamination. The labeling must be in accordance with the SBI Lab Evidence Handling Policy.
8. Record the drive information such as make, model, serial number, number of sectors, number of heads, and jumper settings.
9. With the hard drive removed, boot the evidence computer into the BIOS. If the date and time differ from the actual date and time, note how much they differ.

References:

1. How Computers Work
2. Upgrading and Repairing PCs

Notes:

1. The hard drive from many laptop computers can be removed by using an adapter and imaged with the same procedures as the hard drives removed from desktop computers.
2. Some laptop hard drives can only be removed by trained service personnel and some laptop hard drives have security devices which do not allow them to be used outside of the laptop computer. In these cases, it is permissible to image these computers using the Cable Acquisition Protocol.
3. Marking the cords connecting the hard drive to the evidence computer will allow the examiner to reassemble to computer correctly.

Title: DOS Hard Drive Imaging Protocol
Version: 1.4 (3/9/2010)

Introduction:

This procedure describes the steps to be taken by all personnel of the North Carolina State Bureau of Investigation in imaging hard drives which are evidence in computer forensic examinations, using the Microsoft DOS operating system.

Purpose:

The purpose of this procedure is to use the Microsoft DOS operating system to create a forensic image of evidence hard drives without altering the data on the hard drive.

Equipment:

1. Forensic Tower or Portable Forensic Workstation
2. Prepared Target drive
3. Approved software for forensic imaging
4. Forensic boot disk

Definitions:

1. Evidence drive – Hard drives submitted to the Laboratory as evidence.
2. Forensic boot disk – computer disk containing the MS DOS operating system and a forensic imaging program which is used to boot a computer without altering the data on evidence hard drives.
3. MD5 hash – A 128 bit value that uniquely describes the contents of a file. This is a standard hash value used in computer forensics.
4. SAN – Networked array of hard drives used as a digital evidence repository.
5. Case Folder – A folder located on the SAN for use in a specific investigation, designated by case number.

Calibration:

The forensic towers used in casework must be verified each day that they are used to ensure that the computer hardware and software are functioning properly. The procedure for this verification process can be found in the Digital Evidence Unit Validation and Calibration Manual.

Limitations:

1. Write protection used in the forensic imaging of hard drives can be either hardware or software write protection. The DOS imaging procedure **must** be used to image a hard drive when hardware to write protect the hard drive is not used.
2. While the evidence drive is in the computer and the hard drive is not write protected, the computer must not be booted into Windows. Booting into Windows can change files on the evidence drive.
3. Locking the evidence hard drive ensures that the Target drive cannot be accidentally copied onto the subject's hard drive. Ensure that the subject's hard drive is locked.

4. When using imaging software other than EnCase, care should be used to ensure that the evidence data is not destroyed by copying the Target drive onto the Evidence drive.

Procedures:

1. Insert the evidence drive and the Target drive into the forensic computer.
2. Boot the forensic computer into DOS using a forensic boot disk.
3. Use an approved hashing program to obtain the MD5 hash value of the evidence drive before imaging.
4. Image the evidence hard drive using an approved imaging tool, following the imaging procedures in the product manual.

If imaging in EnCase:

5. Ensure that the evidence drive is locked and unlock the Target drive.
6. EnCase asks if you would like to compress the file. Compression may be used in the imaging of larger hard drives in order to require less CDs or DVDs to store the forensic image at the completion of the analysis.
7. When asked if you would like to do a MD5 hash, choose YES. EnCase used this hash to verify that the Target drive is an exact forensic image of the evidence hard drive.
8. EnCase offers the ability to password protect the forensic image. The decision as to whether or not to use password protection is left to the discretion of the analyst.
9. The Maximum Desired Evidence File Size should be set to 640 Mb if the forensic image is to be saved to CDs. Larger file sizes may be used if the image files will be written to DVDs.
10. In some rare cases, EnCase is unable to create a forensic image of the evidence drive. In this case, other approved imaging programs should be used.
11. After verifying that the forensic image has been successfully completed, remove the subject's hard drive from the forensic computer.

When SAN is available for use:

12. Transfer forensic image file(s) from Target drive to Case Folder on SAN drive.

References:

1. EnCase Forensic User Manual
2. EnCase Intermediate Analysis and Reporting course guide
3. EnCase Advanced Computer Forensics course guide
4. Forensic Toolkit User Guide
5. Forensic Boot Camp Training Manual
6. Digital Evidence Unit Validation and Calibration Manual

Notes:

1. EnCase is the primary imaging tool used by the North Carolina State Bureau of Investigation. Situations may occur when other tools need to be used. In these situations, another imaging tool may be used from the approved list.
2. Making a forensic image of the subject's hard drive is not the same as making a copy of the subject's hard drive. When a hard drive is copied, only the logical files are written to the Target drive. When a forensic image is created of a drive, all of the information on the suspect hard drive is written to the Target drive, including slack space, unallocated space, and deleted files.
3. When working with the hard drive from a laptop computer, the smaller laptop hard drive can be imaged by using the adapter to connect it to the standard IDE connector. The same imaging procedures are used.
4. In most situations, the Windows acquisition is preferable if the hardware allows it. Imaging in Windows is much faster than imaging in DOS.
5. Using compression in EnCase has NO damaging effects on the evidence. These files created are two to three times smaller than uncompressed files. However, creating compressed images may take five times longer than creating uncompressed images.
6. There may be some instances when the subject's hard drive cannot be successfully imaged. In the event that a forensic image cannot be made of the subject's hard drive due to either hardware or software problems, all approved methods of imaging the drive must be exhausted and the attempts to image the hard drive should be completely documented before doing any examination on the subject's original hard drive.

Title: Windows Imaging Protocol
Version: 1.3 (3/9/2010)

Introduction:

This procedure describes the steps to be taken by all personnel of the North Carolina State Bureau of Investigation in imaging hard drives submitted to the Laboratory as evidence, using the Microsoft Windows operating system.

Purpose:

The purpose of this procedure is to use a Microsoft Windows operating system to create a forensic image of evidence hard drives without altering the data on the hard drive.

Equipment:

1. Forensic Tower or Portable Forensic Workstation
2. Prepared Target drive
3. Approved software for forensic imaging

Definitions:

1. Evidence drive – Hard drives submitted to the Laboratory as evidence.
2. MD5 hash – A 128 bit value that uniquely describes the contents of a file. This is the standard hash value used in computer forensics.
3. Forensic drive – Hard drive containing the operating system and all of the forensic software that will be used in the examination.
4. Clone - The process of performing a sector-by-sector copy operation from the suspect drive to the destination drive. The number of sectors copied is determined by the size of the suspect drive.

Calibration:

The forensic towers used in casework must be verified each day that they are used to ensure that the computer hardware and software are functioning properly. The procedure for this verification process can be found in the Digital Evidence Unit Validation and Calibration Manual.

Limitations:

The DOS imaging procedure **must** be used to image a hard drive when hardware to write protect the hard drive is not used.

Procedures:

1. Attach the evidence drive to the forensic computer using a read only hardware device.
2. Insert the forensic drive and Target drive in the forensic computer and boot into Windows.
3. Use an approved hashing program to obtain the MD5 hash value of the evidence drive before imaging.

4. Generate a forensic image of the evidence drive and save it to the Target drive using an approved imaging software program in Windows, following the imaging procedures in the product manual.

If using EnCase:

5. Image the evidence drive by choosing the Acquire button on the tool bar.
6. On the Options screen, enter the case information that the program requests. This information will be used by the program in preparing the EnCase report.
7. Check the check box for Generate image hash. EnCase uses this hash to verify that the Target drive contains an exact forensic image of the evidence drive.
8. EnCase offers the ability to password protect the image.
9. The Maximum Desired Evidence File Size should be set to 640 Mb if the forensic image is to be saved to CDs. Larger file sizes may be used if the forensic image files will be written to DVDs.
10. In some rare cases, EnCase is unable to create a forensic image of the subject's hard drive. In this case, make a clone of the subject's hard drive onto the target drive using other approved imaging software such as SnapBack, or an approved hardware device such as the VOOM HardCopy II.
11. While the subject's hard drive is attached to the read only device, additional programs that require access to the physical disk may be run (i.e. anti-virus software or Net Analysis).
12. After verifying that the forensic image has been successfully completed, remove the subject's hard drive from the forensic computer.

References:

1. EnCase Forensic User Manual
2. EnCase Intermediate Analysis and Reporting course guide
3. EnCase Advanced Computer Forensics course guide
4. Forensic Toolkit User Guide
5. Forensic Boot Camp Training Manual
6. Digital Evidence Unit Validation and Calibration Manual

Notes:

1. EnCase is the primary imaging tool used by the North Carolina State Bureau of Investigation. Situations may occur when other tools need to be used. In these situations, another imaging tool may be used from the approved list.
2. Making a forensic image of the subject's hard drive is not the same as making a copy of the subject's hard drive. When a hard drive is copied, only the logical files are written to the Target drive. When a forensic image is created of a drive, all of the information on the suspect hard drive is written to the Target drive, including slack space, unallocated space, and deleted files.
3. When working with the hard drive from a laptop computer, the smaller laptop hard drive can be imaged by using the adapter to connect it to the standard IDE connector. The same imaging procedures are used.
4. In most situations, the Windows acquisition is preferable if the hardware allows it. Imaging in Windows is much faster than imaging in DOS.

5. The SBI Computer Forensics Unit is equipped with forensic towers having a read only Firewire connection. Hard drives which are connected through validated read-only devices are write protected and may be imaged in the Windows environment.
6. Using compression in EnCase has NO damaging effects on the evidence. These files created are smaller than uncompressed files; however creating compressed images may take longer than creating uncompressed images.
7. There may be some instances when the subject's hard drive cannot be successfully imaged. In the event that a forensic image cannot be made of the subject's hard drive due to either hardware or software problems, all approved methods of imaging the drive must be exhausted and the attempts to image the hard drive should be completely documented before doing any examination on the subject's original hard drive.
8. In instances where the virus scan takes an excessive amount of time to complete, it is permissible to copy all of the logical files out to the Target hard drive and run the scan on these files.
9. Virus definitions on anti-virus software should be updated regularly.

Title: Windows Imaging to SAN Protocol
Version: 1.1 (3/9/2010)

Introduction:

This procedure describes the steps to be taken by all personnel of the North Carolina State Bureau of Investigation in imaging hard drives submitted to the Laboratory as evidence to the SAN, using the Microsoft Windows operating system.

Purpose:

The purpose of this procedure is to use a Microsoft Windows operating system to create a forensic image of evidence hard drives without altering the data on the hard drive.

Equipment:

1. Forensic Tower or Portable Forensic Workstation connected via Fiber cable to SAN storage device
2. Approved software for forensic imaging

Definitions:

1. Evidence drive – Hard drives submitted to the Laboratory as evidence.
2. MD5 hash – A 128 bit value that uniquely describes the contents of a file. This is a standard hash value used in computer forensics.
3. SAN – Networked array of hard drives used as a digital evidence repository.

Calibration:

The forensic towers used in casework must be verified each day that they are used to ensure that the computer hardware and software are functioning properly. The procedure for this verification process can be found in the Digital Evidence Unit Validation and Calibration Manual.

Limitations:

The DOS imaging procedure **must** be used to image a hard drive when hardware to write protect the hard drive is not used.

Procedures:

1. Attach the evidence drive to the forensic computer using a read only hardware device.
2. Use an approved hashing program to obtain the MD5 hash value of the evidence drive before imaging.
3. Generate a forensic image of the evidence drive and save it to the SAN drive using an approved imaging software program in Windows, following the imaging procedures in the product manual.

If using EnCase:

4. Image the evidence drive by choosing the Acquire button on the tool bar.

5. On the Options screen, enter the case information that the program requests. This information will be used by the program in preparing the EnCase report.
6. Check the check box for Generate image hash. EnCase uses this hash to verify that the Target drive contains an exact forensic image of the evidence drive.
7. EnCase offers the ability to password protect the image.
8. The Maximum Desired Evidence File Size should be set to 640 Mb if the forensic image is to be saved to CDs. Larger file sizes may be used if the forensic image files will be written to DVDs.
9. In some rare cases, EnCase is unable to create a forensic image of the subject's hard drive. In this case, make a forensic copy of the subject's hard drive onto a prepared target drive using other approved imaging software such as SnapBack, or an approved hardware device such as the VOOM HardCopy II. Make a forensic image of the target drive onto the SAN drive using an approved imaging software program in Windows, following the imaging procedures in the product manual.
10. While the subject's hard drive is attached to the read only device, additional programs that require access to the physical disk may be run (i.e. anti-virus software or Net Analysis).
11. After verifying that the forensic image has been successfully completed, remove the subject's hard drive from the forensic computer.

References:

1. EnCase Forensic User Manual
2. EnCase Intermediate Analysis and Reporting course guide
3. EnCase Advanced Computer Forensics course guide
4. Forensic Toolkit User Guide
5. Forensic Boot Camp Training Manual
6. Digital Evidence Unit Validation and Calibration Manual

Notes:

1. EnCase is the primary imaging tool used by the North Carolina State Bureau of Investigation. Situations may occur when other tools need to be used. In these situations, another imaging tool may be used from the approved list.
2. Making a forensic image of the subject's hard drive is not the same as making a copy of the subject's hard drive. When a hard drive is copied, only the logical files are written to the Target drive. When a forensic image is created of a drive, all of the information on the suspect hard drive is written to the Target drive, including slack space, unallocated space, and deleted files.
3. When working with the hard drive from a laptop computer, the smaller laptop hard drive can be imaged by using the adapter to connect it to the standard IDE connector. The same imaging procedures are used.
4. In most situations, the Windows acquisition is preferable if the hardware allows it. Imaging in Windows is much faster than imaging in DOS.
5. The SBI Computer Forensics Unit is equipped with forensic towers having a read only Firewire connection. Hard drives which are connected through

validated read-only devices are write protected and may be imaged in the Windows environment.

6. Using compression has NO damaging effects on the evidence. These files created are two to three times smaller than uncompressed files. However, creating compressed images may take five times longer than creating uncompressed images.
7. There may be some instances when the subject's hard drive cannot be successfully imaged. In the event that a forensic image cannot be made of the subject's hard drive due to either hardware or software problems, all approved methods of imaging the drive must be exhausted and the attempts to image the hard drive should be completely documented before doing any examination on the subject's original hard drive.
8. In instances where the virus scan takes an excessive amount of time to complete, it is permissible to copy all of the logical files out to the hard drive and run the scan on these files.
9. Virus definitions on anti-virus software should be updated regularly.

Title: Cable Acquisition Protocol
Version: 1.4 (3/9/2010)

Introduction:

This procedure describes the steps to be taken by all personnel of the North Carolina State Bureau of Investigation in imaging computers using a null-modem parallel (laplink) cable or network crossover cable.

Purpose:

The purpose of this procedure is to image evidence drives still installed in the evidence computers in a situation where the hard drive is difficult or impossible to remove. This protocol provides a procedure for imaging these computers without making changes to the data on the evidence drive.

Equipment:

1. Forensic Tower or Portable Forensic Workstation
2. Prepared Target drive
3. EnCase boot floppy

Definitions:

1. Target Drive – the drive that information from the suspect drive is being written to.
2. Evidence Drive - Hard drives submitted to the Laboratory as evidence.
3. EnCase boot floppy - a 3 ½ inch computer disk containing the MS DOS operating system and a copy of the EnCase forensic imaging program which is used to boot a computer without altering the data on evidence hard drives.
4. Server mode – DOS mode that the suspect computer is put into to enable it to send data to a forensic computer in a forensically safe manner for imaging.
5. Clientmode - DOS mode that the forensic computer is put into to enable it to receive data from an evidence computer in a forensically safe manner for imaging.
6. SAN – Networked array of hard drives used as a digital evidence repository.
7. Case Folder – A folder located on the SAN for use in a specific investigation, designated by case number.

Calibration:

The forensic towers used in casework must be verified each day that they are used to ensure that the computer hardware and software are functioning properly. The procedure for this verification process can be found in the Digital Evidence Unit Validation and Calibration Manual.

Limitations:

1. Always set up the evidence computer in server mode first.
2. If possible, check the evidence computer prior to booting to ensure that the boot order is to the floppy drive first. Also, disable any power saving features in the BIOS.

Procedures:

1. Set up the evidence computer in server mode by booting into DOS using an EnCase boot floppy.
2. Connect the evidence computer and forensic computer using a network crossover cable between the network interface cards or connect the laplink cable from the parallel port of the evidence computer to the parallel port of the forensic computer (running through the dongle if a parallel port dongle is used).
3. Once the evidence computer has booted, run EnCase in DOS.
4. The evidence computer will display its hard drive information on the screen and you will note that the evidence drive is locked.
5. Choose “server mode” from the choices at the bottom of the screen.
6. A window will be displayed showing “Server Mode” and the message “waiting to connect”.
7. Install the Target drive into the forensic computer.
8. Set up the forensic computer in client mode by booting the forensic computer into DOS using an EnCase forensic boot disk and running EnCase.
9. Ensure that the screen in of the forensic computer shows “client mode” in the title bar.
10. The information that you now see on the screen will be from the evidence computer.
11. The evidence drive can now be acquired by following the steps in the **DOS Hard Drive Imaging Protocol**.
12. Prior to imaging the hard drive, use an approved hashing program to obtain the MD5 hash value of the evidence drive before imaging.
13. When acquisition has started, the server (suspect) computer window will show that a connection has been established and the data being transferred.

When SAN is available for use:

14. Transfer forensic image file(s) from Target drive to Case Folder on SAN drive.

References:

1. EnCase Forensic User Manual
2. EnCase Intermediate Analysis and Reporting course guide
3. EnCase Advanced Computer Forensics course guide
4. Digital Evidence Unit Validation and Calibration Manual

Notes:

1. EnCase is the primary imaging tool used by the North Carolina State Bureau of Investigation. Situations may occur when other tools need to be used. In these situations, another imaging tool may be used from the approved list.
2. In order to use a network crossover cable, the suspect computer must be equipped with a network interface card and the forensic boot disk must contain the DOS drivers for that network interface card. Otherwise, the parallel cable must be used.

3. This is a very slow method of data acquisition. Using a network crossover cable is a faster method of imaging a hard drive than using a parallel cable. A hard drive greater than 20 GB in size may take several days to acquire using a parallel cable.

Title: Removable/External Media Imaging Protocol
Version: 1.4 (3/9/2010)

Introduction:

This procedure describes the steps to be taken by all personnel of the North Carolina State Bureau of Investigation in imaging various types of removable media which may be submitted to the Laboratory.

Purpose:

The purpose of this procedure is to image various types of removable media, including floppy disks, CDs, DVDs, MP3 players, Zip disks, Jazz disks, LS120 disks, digital cameras and flash memory cards, without making changes to the data on the media.

Equipment:

1. Forensic Tower or Portable Forensic Workstation
2. Prepared Target drive

Definitions:

Target Drive – the drive that holds the forensic image of the suspect drive and the case file containing any evidence found on the suspect drive.

Calibration:

The forensic towers used in casework must be verified each day that they are used to ensure that the computer hardware and software are functioning properly. The procedure for this verification process can be found in the Digital Evidence Unit Validation and Calibration Manual.

Limitations:

1. When a case is submitted to the laboratory that contains a PDA, great care should be taken to ensure that the batteries do not go dead. The volatile memory in a PDA can be lost when the batteries are totally discharged. PDAs which use AA or AAA batteries should have new batteries placed into the PDA. PDAs with rechargeable batteries should be charged if the charger is submitted. If these things cannot be done to ensure the safety of the evidence on the PDA, the evidence should be imaged and then worked at the appropriate time.

Procedures:

1. If possible, write protect any removable media.
2. The evidence can be imaged to a blank copy of the same media type. The original media should be labeled as the original, and the duplicates should be used for examination.
3. If using EnCase for the examination, the removable media can be added to the case and imaged to the Target drive.
4. If the media can be write protected and keyword searches are not needed on the media, it is permissible to preview the original media without making a forensic image first.

References:

1. EnCase Forensic User Manual
2. EnCase Intermediate Analysis and Reporting course guide
3. EnCase Advanced Computer Forensics course guide
4. Forensic Toolkit User Guide
5. Forensic Boot Camp Training Manual
6. Digital Evidence Unit Validation and Calibration Manual

Notes:

1. If working with a subject's CD-R or CD-RW disks, reading them in read only CD drives is preferred. This will prevent changes from being made to the evidence. The Sony CD-R/DVD-R drive installed on the computer forensic unit’s forensic towers has been validated to ensure that changes will not be made to evidence media.
2. Hard drives must only be imaged in DOS if write protection hardware is not in use. Likewise, removable media which can be write protected, can be imaged in the Windows based EnCase program.
3. When batch imaging floppy disks, EnCase chooses the disk capacity of the first floppy imaged as the capacity of all floppies in the batch. If a double density disk is imaged first, EnCase will not see all of the data on any high density disks which are imaged later in the batch.
4. EnCase has problems reading the format used by some computers to write to CD-RW disks. If a CD-RW is imaged or previewed in EnCase and shows no data on the disk, the disk may be examined in Windows Explorer. If there is data on the disk and EnCase doesn’t recognize it, Windows Explorer will read it. If a disk is found that contains data but is not recognized by EnCase, this disk may be examined with CD\DVD Inspector or another approved imaging program. If the data is still not viewable, the data on the disk should be copied to a CD-R disk and this copy used in EnCase. It should be noted that this method will only capture the Logical files on the CD-RW, and not the deleted files or slack space.
5. Media Specific Notes:
   - <u>Floppy Disks</u>
     High density and double density floppy disks should be batched and imaged separately.
   - <u>CDs</u>
     When using EnCase to image CD-RW disks, care must be taken to ensure that EnCase can read the data on the disk. (See note 4)
   - <u>Zip Disks</u>
     Zip disks cannot themselves be write protected and should be imaged in DOS or imaged using hardware or software write protection.
   - <u>PDAs</u>
     For PDA examination, a docking cradle made for the particular make and model of PDA is required. When the PDA is attached to the forensic tower using the cradle, EnCase see the PDA as a piece of removable media. The

data contained on the PDA can then be acquired by EnCase in the same method as with any other type of removable media.

- Digital Cameras
  For examination of digital cameras, the flash memory cards should be removed from the camera. A flash media card reader is used to read the data on the media. EnCase sees the flash media as a piece of removable media. The data contained on the flash media card can then be acquired by EnCase in the same method as with any other type of removable media. If an adapter cable is available, the internal memory of the camera should also be examined using approved forensic software.

Title: Removable/External Media Imaging to SAN Protocol
Version: 1.1 (3/9/2010)

Introduction:
This procedure describes the steps to be taken by all personnel of the North Carolina State Bureau of Investigation in imaging various types of removable media which may be submitted to the Laboratory.

Purpose:
The purpose of this procedure is to image various types of removable media, including floppy disks, CDs, DVDs, MP3 players, Zip disks, Jazz disks, LS120 disks, digital cameras and flash memory cards, without making changes to the data on the media.

Equipment:

1. Forensic Tower or Portable Forensic Workstation
2. Online SAN drive

Definitions:
SAN – Networked array of hard drives used as a digital evidence repository.

Calibration:
The forensic towers used in casework must be verified each day that they are used to ensure that the computer hardware and software are functioning properly. The procedure for this verification process can be found in the Digital Evidence Unit Validation and Calibration Manual.

Limitations:

1. When a case is submitted to the laboratory that contains a PDA, great care should be taken to ensure that the batteries do not go dead. The volatile memory in a PDA can be lost when the batteries are totally discharged. PDAs which use AA or AAA batteries should have new batteries placed into the PDA. PDAs with rechargeable batteries should be charged if the charger is submitted. If these things cannot be done to ensure the safety of the evidence on the PDA, the evidence should be imaged and then worked at the appropriate time.

Procedures:

1. If possible, write protect any removable media.
2. The evidence can be imaged to a blank copy of the same media type. The original media should be labeled as the original, and the duplicates should be used for examination.
3. If using EnCase for the examination, the removable media can be added to the case and imaged to the SAN drive.
4. If the media can be write protected and keyword searches are not needed on the media, it is permissible to preview the original media without making a forensic image first.

References:

1. EnCase Forensic User Manual
2. EnCase Intermediate Analysis and Reporting course guide
3. EnCase Advanced Computer Forensics course guide
4. Forensic Toolkit User Guide
5. Forensic Boot Camp Training Manual
6. Digital Evidence Unit Validation and Calibration Manual

Notes:

1. If working with a subject's CD-R or CD-RW disks, reading them in read only CD drives is preferred. This will prevent changes from being made to the evidence. The Sony CD-R/DVD-R drive installed on the computer forensic unit's forensic towers has been validated to ensure that changes will not be made to evidence media.
2. Hard drives must only be imaged in DOS if write protection hardware is not in use. Likewise, removable media which can be write protected, can be imaged in the Windows based EnCase program.
3. When batch imaging floppy disks, EnCase chooses the disk capacity of the first floppy imaged as the capacity of all floppies in the batch. If a double density disk is imaged first, EnCase will not see all of the data on any high density disks which are imaged later in the batch.
4. EnCase has problems reading the format used by some computers to write to CD-RW disks. If a CD-RW is imaged or previewed in EnCase and shows no data on the disk, the disk should be examined in Windows Explorer. If there is data on the disk and EnCase doesn't recognize it, Windows Explorer will read it. If a disk is found that contains data but is not recognized by EnCase, this disk should be examined with CD\DVD Inspector or another approved imaging program. If the data is still not viewable, the data on the disk should be copied to a CD-R disk and this copy used in EnCase. It should be noted that this method will only capture the Logical files on the CD-RW, and not the deleted files or slack space.
5. Media Specific Notes:

   <u>Floppy Disks</u>

   High density and double density floppy disks should be batched and imaged separately.

   <u>CDs</u>

   When using EnCase to image CD-RW disks, care must be taken to ensure that EnCase can read the data on the disk. (See note 4, below)

   <u>Zip Disks</u>

   Zip disks cannot themselves be write protected and should be imaged in DOS or imaged using hardware or software write protection.

   <u>PDAs</u>

   For PDA examination, a docking cradle made for the particular make and model of PDA is required. When the PDA is attached to the forensic tower using the cradle, EnCase see the PDA as a piece of removable media. The data contained on the PDA can then be acquired by EnCase in the same method as with any other type of removable media.

Digital Cameras

For examination of digital cameras, the flash memory cards should be removed from the camera. A flash media card reader is used to read the data on the media. EnCase sees the flash media as a piece of removable media. The data contained on the flash media card can then be acquired by EnCase in the same method as with any other type of removable media. If an adapter cable is available, the internal memory of the camera should also be examined using approved forensic software.

Title: M26 Taser Data Download Protocol
Version: 1.1 (8/1/2008)

Introduction:
This procedure describes the steps to be taken by all personnel of the North Carolina State Bureau of Investigation in downloading the firing data from M26 model Tasers.

Purpose:
The purpose of this procedure is to retrieve the firing data from M26 Tasers that are submitted to the Laboratory for analysis. This protocol provides a procedure for downloading this data without making changes to the data on the Taser.

Equipment:

1. Forensic Tower
2. M26 dataport download kit from Taser International

Definitions:
M26 dataport download kit – kit containing the hardware and software needed to download the firing information from an M26 Taser.

Calibration:
The forensic towers used in casework must be verified each day that they are used to ensure that the computer hardware and software are functioning properly. The procedure for this verification process can be found in the Digital Evidence Unit Validation and Calibration Manual.

Precautions:

1. M26 Tasers are high energy weapons and should be handled with great care.
2. If a live cartridge is attached to the front of the weapon, it has the ability to discharge sharp projectiles. These cartridges should be removed from weapons submitted for examination.
3. The M26 Taser can still deliver an electrical shock with the cartridge removed. Analysts should keep the safety engaged whenever possible, keep his or her finger off of the trigger whenever possible, and avoid touching the electrodes on the front of the weapon.

Limitations:

1. The M26 data log shows the trigger pulls in increments of 5 seconds. If the user pulls the trigger once and releases it, the M26 will fire for five seconds and the data log will show one firing. If the user pulls the trigger and holds it for longer than 5 seconds, the unit will continue to fire and the data log will show multiple firings. For example, if the user pulls and holds the trigger longer than 5 seconds but less than 10 seconds, the data log will show two firings. If the user pulls and holds the trigger longer than 10 seconds but less than 15 seconds, the data log will show three firings.

2. There is no record of time changes stored on the M26, as there is with the X26. If the user changes the time on the M26, the time change will be reflected in the next firing entry, but there is no record stored when the user changes the time.

Procedures:

1. Install the software from the M26 dataport download kit on the forensic tower if it is not already installed.
2. Verify that the time and time zone information on the forensic tower are correct.
3. To begin the acquisition process, the Taser must have the safety engaged, the batteries must be in unit, and the Data Port Plug must be removed.
4. Connect one end of the 9 Pin serial cable to the serial port of the forensic tower and the other end to the interface box.
5. Connect one end of the interface cable (blue cable) to the interface box and the other end to M26 Taser data Port. The light on the interface box will light up (green light) while the light on the M26 Taser will (depending on the charge in the batteries) blink three times before staying lit or continue to blink.
6. Open the Taser interface program and enter the number of the comm port that the Taser is connected to and the password. The password can be found written on the outside of the diskette in the M26 download kit.
7. Download the firing data.
8. Save the firing data to a file on the Forensic Tower.

References:

1. Operational Use of Logging Program V2.0 (found as the readme file on the diskette in the M26 download kit)
2. Digital Evidence Unit Validation and Calibration Manual

Notes:

1. The following firing information will be displayed for the Taser: Line #, date mm/dd/yy, time in military time, and day of the week for each discharge.
2. During verification testing, when the trigger on the Taser was held for more than 5 seconds, there were intermittent errors in the firing data (time incrementing by 6 minutes on a 10-second trigger pull, a 7-second trigger pull with only one entry instead of two, and an incorrect date on an entry for a 12-second trigger pull).

Title: X26 Taser Data Download Protocol
Version: 1.3 (3/9/2010)

Introduction:

This procedure describes the steps to be taken by all personnel of the North Carolina State Bureau of Investigation in downloading the firing data from X26 model Tasers.

Purpose:

The purpose of this procedure is to retrieve the firing data from X26 Tasers that are submitted to the Laboratory for analysis. This protocol provides a procedure for downloading this data without making changes to the data on the Taser.

Equipment:

1. Forensic Tower
2. USB data interface module from Taser International

Definitions:

1. USB data interface module – kit containing the hardware and software needed to download the firing information from an X26 Taser.
2. USB DPM – connector from the interface module which plugs into the battery compartment of the X26 Taser.

Calibration:

The forensic towers used in casework must be verified each day that they are used to ensure that the computer hardware and software are functioning properly. The procedure for this verification process can be found in the Digital Evidence Unit Validation and Calibration Manual.

Precautions:

1. X26 Tasers are high energy weapons and should be handled with great care.
2. If a live cartridge is attached to the front of the weapon, it has the ability to discharge sharp projectiles. These cartridges should be removed from weapons submitted for examination.
3. The X26 Taser can still deliver an electrical shock with the cartridge removed. Analysts should keep the safety engaged whenever possible, keep his or her finger off of the trigger whenever possible, and avoid touching the electrodes on the front of the weapon.

Limitations:

None

Procedures:

1. Install the software from the USB data interface module on the forensic tower if it is not already installed.
2. Verify that the time and time zone information on the forensic tower are correct.

3. Ensure the X26 safety switch is in the ON (SAFE) position and remove the air cartridge.
4. Insert the USB cable into the computer. The USB DPM will illuminate red if the cable is connected correctly.
5. Insert the USB DPM into the X26 Taser. After a few seconds the USB DPM illumination will change from red to green and a “U” will appear on the X26 CID.
6. Click on the “Taser X26 Dataport” desktop icon.
7. Check the Daylight Savings Time zone box if your time zone is currently on daylight savings time.
8. Click the “Download X26” button[1].
9. Select a range of dates to download, or choose “Download all firing data” and click continue.
10. Save the firing data to a file on the Forensic Tower.

References:

1. Taser International Data Port User Manual V.15.5
2. Digital Evidence Unit Validation and Calibration Manual

Notes:

1. The following firing information will be displayed for the Taser: Sequence #, GMT time, local time, duration (Secs), Temperature (deg. C), and battery % for each discharge.
2. The X26 shows the total time in seconds that the trigger was pulled. If the user pulls the trigger once and releases it, the X26 will shoot a 5 second burst and 5 seconds will display on the data log. If the user manually turns off firing before a full 5 seconds has elapsed, the number of seconds that the unit fired will display on the data log. If the user pulls the trigger and holds it for longer than 5 seconds, the unit will continue to fire and the total number of seconds the trigger is held will display on the data log.
3. Duration is the total time the trigger was depressed without a break.
4. The temperature is the internal DPM temperature.
5. The Time Change Record is a log of all changes to the Taser’s internal clock. If the internal clock has never been updated, the area is blank.
6. If the time on the computer does not match the time on the X26, a “Time Synchronization error” window will appear. If this happens, press the cancel button. **DO NOT change the time on the X26 Taser**.
7. If no “Time Synchronization error” window is displayed after the “Download X26” button has been pressed, the Taser’s internal clock must be checked. To check the Taser’s internal clock the software must be exited after all data downloads are complete. The forensic workstation’s clock may be set either forwards or backwards 12 hours to produce a

[1] See notes 6 and 7 for procedures to follow based on the resulting screen after the “Download X26” button is pressed.

“Time Synchronization error”. Restart the software and press the “Download X26” button. Compare the time displayed as the Taser’s internal clock setting to actual time (from DOJ Internal Network clock setting) and record the difference (if any).

Title: Taser Function Test Protocol
Version: 1.1 (8/1/2008)

Introduction:

This procedure describes the steps to be taken by all personnel of the North Carolina State Bureau of Investigation in function testing M26 and X26 model Tasers.

Purpose:

The purpose of this procedure is to test Tasers that are submitted for analysis to ensure that they are recording the firing information properly.

Equipment:

1. Forensic Tower
2. M26 dataport download kit from Taser International
3. USB data interface module from Taser International

Definitions:

1. M26 dataport download kit – kit containing the hardware and software needed to download the firing information from an M26 Taser.
2. USB data interface module – kit containing the hardware and software needed to download the firing information from an X26 Taser.

Calibration:

The forensic towers used in casework must be verified each day that they are used to ensure that the computer hardware and software are functioning properly. The procedure for this verification process can be found in the Digital Evidence Unit Validation and Calibration Manual.

Precautions:

1. Tasers are high energy weapons and should be handled with great care.
2. If a live cartridge is attached to the front of the weapon, it has the ability to discharge sharp projectiles. These cartridges should be removed from weapons submitted for examination.
3. The Taser can still deliver an electrical shock with the cartridge removed. Analysts should keep the safety engaged whenever possible, keep his or her finger off of the trigger whenever possible, and avoid touching the electrodes on the front of the weapon.

Limitations:

1. The M26 data log shows the trigger pulls in increments of 5 seconds. If the user pulls the trigger once and releases it, the M26 will fire for five seconds and the data log will show one firing. If the user pulls the trigger and holds it for longer than 5 seconds, the unit will continue to fire and the data log will show multiple firings. For example, if the user pulls and holds the trigger longer than 5 seconds but less than 10 seconds, the data log will show two firings. If the user pulls and

holds the trigger longer than 10 seconds but less than 15 seconds, the data log will show three firings.

Procedures:

1. Install the download software for the Taser model to be tested on the forensic tower if it is not already installed.
2. Verify that the time and time zone information on the forensic tower are correct.
3. Download the firing data from the weapon to be tested using the procedures in the M26 Acquisition Protocol or the X26 Acquisition Protocol (if the data has not been downloaded while working the case).
4. Set the time on the Forensic Tower to match the time on the Taser.
5. Remove the Taser from the Forensic Tower.
6. Replace the battery pack into an X26 Taser.
7. Discharge the weapon by pulling the trigger and holding it for less than 5 seconds. Record the time that the discharge occurred and the length of time that the trigger was held.
8. Discharge the weapon by pulling the trigger and holding it for more than 5 seconds but less than 10 seconds. Record the time that the discharge occurred and the length of time that the trigger was held.
9. Discharge the weapon by pulling the trigger and holding it for more than 10 seconds. Record the time that the discharge occurred and the length of time that the trigger was held.
10. Download the firing data from the weapon to being tested using the procedures in the M26 Acquisition Protocol or the X26 Acquisition Protocol.
11. Compare the known discharge time and durations to the discharge times and durations recorded on the Taser.
12. Compare the download data from before the function test and the download data from after the function test. Ensure that none of the information on previous firings changed during the function test.

References:

1. Operational Use of Logging Program V2.0 (found as the readme file on the diskette in the M26 download kit)
2. Taser International Data Port User Manual V.15.5
3. Digital Evidence Unit Validation and Calibration Manual

Notes:

None

Title: Mac Preview Protocol
Version: 1.1 (8/1/2008)

Introduction:
This procedure describes the steps to be taken by all personnel of the North Carolina State Bureau of Investigation in previewing computers running the Apple Macintosh operating system, submitted to the Laboratory as evidence, using the HELIX Linux operating system.

Purpose:
The purpose of this procedure is to use the HELIX Linux operating system to preview evidence hard drives without altering the data on the hard drive.

Equipment:

1. Forensic Tower
2. FireWire (IEEE 1394) cable
3. HELIX CD
4. Prepared target drive (as needed)

Definitions:

1. FireWire Target Mode – FireWire Target Mode allows a Mac system to act as if the entire computer were an external FireWire hard drive for another system. This mode works at the firmware level before the operating system is engaged and booted. It is entered by holding down the "T" key on the Mac system during the boot process.
2. HELIX – HELIX is a Linux operating system variant that was specially constructed for forensic examination of live systems due to the fact that all media on the system is placed in read-only mode.
3. `fstab` – `fstab` is a configuration file that contains information for all of the partitions and storage devices in a Linux-based computer. `fstab` contains information concerning how and where the partitions and storage devices in a Linux-based system should be mounted.
4. HFS - Hierarchical File System (HFS) is a file system developed by Apple for use in computers running Mac OS. HFS is also referred to as Mac OS Standard.
5. HFS+ - HFS Plus or HFS+ is a file system developed by Apple to replace their Hierarchical File System (HFS) as the primary file system used in Macintosh computers (or other systems running Mac OS). HFS Plus is an improved version of HFS, supporting much larger files (block addresses are 32-bit length instead of 16-bit) and using Unicode for naming the file items. HFS Plus also uses a full 32-bit allocation mapping table, rather than HFS's 16 bits. HFS Plus is also referred to as Mac OS Extended.

Calibration:
The forensic towers used in casework must be validated each day that they are used to ensure that the computer hardware and software are functioning properly. The

procedure for this validation process can be found in the Digital Evidence Unit Validation and Calibration Manual.

Precautions:

1. **NEVER** use a Microsoft Windows operating system to preview or image a Macintosh system FireWire connection. Microsoft operating systems “touch” drives during the boot sequence. Furthermore, FireWire connections cannot be write-protected so there is no way to prevent writes to the Mac system when mounted to a Windows OS.
2. If you are using another Mac as the examination platform, make sure that you turn off DiskArbitration otherwise there may be inadvertent writes to the suspect Mac system.

Limitations:

1. Be sure to plug in a power cable to any MacBook or other Macintosh laptop to be previewed. Do not allow a laptop to run on battery power during a preview or acquisition if the appropriate AC power cord is available.

Procedures:

1. With both systems powered off, connect the forensic tower to the Mac using a FireWire cable.
2. Boot up the Mac and hold down the "T" key until you see a screen with a FireWire logo floating around to place the Mac into FireWire Target Mode.
3. Boot the forensic tower into the HELIX environment.
4. When the HELIX environment has fully loaded, open up a terminal session.
5. Navigate to the `/etc` directory.
6. Edit the `fstab` file. Navigate to the entry in the `fstab` file that corresponds to the HFS partition on the Mac’s hard drive and change the partition type from “`hfs`” to “`hfsplus`”.
7. If there is a need to copy data off of the Mac during the preview, the target drive must be mounted as read/write in the `fstab` file by changing the "ro" characteristic (Read-Only) to "rw" (Read-Write).
8. Close the terminal session.
9. On the HELIX desktop, click once on the Mac hard drive icon to mount the drive. Repeat this process for the target drive (if used) to mount the target drive.
10. Preview the Mac system using the tools of choice.
11. At the completion of the preview, power down the Mac and disconnect the FireWire cable between the two systems.

References:

1. Digital Evidence Unit Validation and Calibration Manual

Notes:

1. The changes to the fstab file allow the HELIX environment to properly read the file system on newer Macintosh systems while remaining in a read-only state.

2. The industry standard best practice for examining a Macintosh system is to boot the Mac into FireWire Target mode because this mode engages at the firmware level before the operating system is booted. To enter FireWire Target Mode boot the Mac and hold down the "T" key until a screen with a floating FireWire logo is seen.

Title: Evidence Search Protocol
Version: 1.3 (3/9/2010)

Introduction:
This procedure describes the steps to be taken by all personnel of the North Carolina State Bureau of Investigation in searching computer evidence that is submitted to the Laboratory.

Purpose:
The purpose of this procedure is to provide a systematic means of searching digital evidence in order find the data of interest.

Equipment:

1. Forensic Tower or Portable Forensic Workstation
2. Approved Forensic Software

Definitions:

1. Forensic drive - Hard drive containing the operating system and all of the forensic software that will be used in the examination
2. Target drive - the drive that holds the forensic image of the suspect drive and the case file containing any evidence found on the suspect drive.

Calibration:
The forensic towers used in casework must be verified each day that they are used to ensure that the computer hardware and software are functioning properly. The procedure for this verification process can be found in the Digital Evidence Unit Validation and Calibration Manual.

Limitations:
None

Procedures:

1. Install the forensic drive and the target drive into the forensic tower.
2. Ensure that the forensic drive is installed as the primary master and the target drive is installed as either the primary slave, secondary master, or secondary slave.
3. Boot the forensic tower from the forensic drive.
4. Run approved software to undelete any deleted files and recover files and file fragments from unallocated space.
5. The forensic image of the evidence drive should be examined for the presence of any deleted partitions on the hard drive. If any deleted partitions are noted, these partitions should be recovered.
6. The forensic image of the evidence drive should be examined for the presence of any deleted folders on the hard drive. Any deleted folders should be recovered.
7. If using EnCase, a file mounter enscript should be run to mount any zipped or compressed files so that the files contained inside can be examined.

8. A signature analysis should be run on all of the files in the case prior to the examination of these files. The signature analysis checks the file header information to ensure that the files have not been misidentified with an incorrect file extension.

For Cases Involving Images

1. Computer search software or graphics thumbnail software can be used to view images on a forensic image.
2. A file search can be run to find files with graphics or movie file extensions (.jpg, .gif, .bmp, .mov, .mpg, .avi, etc.).
3. Examine files found for data useful to the investigation.
4. Make note of any files found with valuable information.

Data Searches

1. Use approved forensic search software to perform keyword searches on the forensic image.
2. Enter in keywords such as names, e-mail addresses, dates, or other pertinent keywords which may be used in a file containing data of evidentiary value.
3. Examine files found for data useful to the investigation.
4. Make note of any files found with valuable information.

Image Restore

1. At times, it will be necessary to view the subject’s computer just as they would have viewed it at the time it was in use. To do this, it is acceptable to image the drive again with an approved DOS based imaging program such as SnapBack or to use the restore function in EnCase to restore the EnCase image to a target hard drive. This second image can then be used to boot the subject’s computer.

References:

1. EnCase Forensic User Manual
2. EnCase Intermediate Analysis and Reporting course guide
3. EnCase Advanced Computer Forensics course guide
4. Forensic Toolkit User Guide
5. Forensic Boot Camp Training Manual
6. Digital Evidence Unit Validation and Calibration Manual

Notes:

1. In EnCase .asf, .max, .mpe, .mpeg, .mpg, .mov, .rm, .ram and .avi files as well as image files in unallocated space are not shown in the gallery view. These files should be searched for and viewed with external viewers.
2. EnCase does not display images inside of .zip files in the gallery view unless the zip files are first mounted. The examiner should search for .zip files. These files should be opened manually or with the File mounter EnScript in EnCase and any images found inside examined. This can be done by the examiner or recovered for examination by the submitting officer.
3. EnCase does not display images that are attached to e-mail files (i.e. Outlook Express and AOL e-mail files) prior to version 5. If images may be important in a case and an Encase version prior to version 5 is being used, the e-mail files

should be recovered to the target drive. These files can be examined by restoring the e-mails to an e-mail account on another computer so that the images attached to the e-mail can be viewed. This examination can be done by the examiner or recovered for examination by the submitting officer. Alternatively, the examiner may use another tool such as Forensic Tool Kit to examine the case for e-mail.

4. Due to the size of modern hard drives, it is not possible to read all of the data recovered in a case. Every effort should be made to search by relevant dates or file types and search by relevant keywords in order to find information pertinent to the case.
5. Microsoft Office 2007 documents are different than previous versions. The following was copied from the Guidance Software website:
   “*Microsoft's Office 2007 documents are stored in what is referred to as the Office Open XML File Format. It is a ZIP file of various XML documents describing the entire document.”*
   In order to view the contents of these files, they must be mounted like other types of Zip files.
   When using version 5 of EnCase, mounting ZIP files will allow you to see the contents of Office 2007 documents.
   When using version 6 of EnCase, you must select “Mount Persistant” option inside of the File Mounter EnScript to keep the files mounted after the EnScript completes running. If you do not select this option, the files will unmount as soon as the EnScript finishes running and you will manually have to mount the files by right clicking and viewing file structure.

Title: Evidence Search (SAN) Protocol
Version: 1.1 (3/9/2010)

Introduction:
This procedure describes the steps to be taken by all personnel of the North Carolina State Bureau of Investigation in searching computer evidence that is submitted to the Laboratory.

Purpose:
The purpose of this procedure is to provide a systematic means of searching digital evidence in order find the data of interest.

Equipment:
1. Forensic Virtual Machine
2. Approved Forensic Software

Definitions:
1. Forensic drive - Hard drive containing the operating system and all of the forensic software that will be used in the examination
2. SAN – Networked array of hard drives used as a digital evidence repository.
3. Virtual Machine (VM) – A software emulation of a computer that executes programs like a real machine.
4. Case Folder – A folder located on the SAN for use in a specific investigation, designated by case number.

Calibration:
The Virtual Machines used in casework must be verified each day that they are used to ensure that the software is functioning properly. The procedure for this verification process can be found in the Digital Evidence Unit Validation and Calibration Manual.

Limitations:
In order to prevent cross-contamination from within Virtual Machines, the following steps must be taken during the deployment of a new virtual machine from a template virtual machine.
1. While in the VM Configuration, under the Shared Folders menu, uncheck “Share Mac OS X folders with windows” and “Share all Windows disks with Mac OS X”. Check the “Map folders to drive letters” and “User-defined Mac OS X folders” and set the folder path to: /Desktop/*case folder #*. This ensures that a single VM can only see the files associated with one case, preventing inadvertent file access.

Procedures:
1. Connect to SAN node with analyst workstation.
2. Deploy a new Forensic Virtual Machine from a template and map a path to the Case Folder from the VM.

3. Run approved software to undelete any deleted files and recover files and file fragments from unallocated space.
4. The forensic image of the evidence drive should be examined for the presence of any deleted partitions on the hard drive. If any deleted partitions are noted, these partitions should be recovered.
5. If the evidence drive used a FAT file system, the forensic image of the evidence drive should be examined for the presence of any deleted folders on the hard drive. Any deleted folders should be recovered.
6. If using EnCase, a file mounter enscript should be run to mount any zipped or compressed files so that the files contained inside can be examined.
7. A signature analysis should be run on all of the files in the case prior to the examination of these files. The signature analysis checks the file header information to ensure that the files have not been misidentified with an incorrect file extension.

For Cases Involving Images

1. Computer search software or graphics thumbnail software can be used to view images on a forensic image.
2. A file search can be run to find files with graphics or movie file extensions (.jpg, .gif, .bmp, .mov, .mpg, .avi, etc.).
3. Examine files found for data useful to the investigation.
4. Make note of any files found with valuable information.

Data Searches

1. Use approved forensic search software to perform keyword searches on the forensic image.
2. Enter in keywords such as names, e-mail addresses, dates, or other pertinent keywords which may be used in a file containing data of evidentiary value.
3. Examine files found for data useful to the investigation.
4. Make note of any files found with valuable information.

Image Restore

1. At times, it will be necessary to view the subject’s computer just as they would have viewed it at the time it was in use. To do this, it is acceptable to image the drive again with an approved DOS based imaging program such as SnapBack or to use the restore function in EnCase to restore the EnCase image to a target hard drive. This second image can then be used to boot the subject’s computer.

References:

1. EnCase Forensic User Manual
2. EnCase Intermediate Analysis and Reporting course guide
3. EnCase Advanced Computer Forensics course guide
4. Forensic Toolkit User Guide
5. Forensic Boot Camp Training Manual
6. Digital Evidence Unit Validation and Calibration Manual

Notes:

1. In EnCase .asf, .max, .mpe, .mpeg, .mpg, .mov, .rm, .ram and .avi files as well as image files in unallocated space are not shown in the gallery view. These files should be searched for and viewed with external viewers.
2. EnCase does not display images inside of .zip files in the gallery view unless the zip files are first mounted. The examiner should search for .zip files. These files should be opened manually or with the File mounter EnScript in EnCase and any images found inside examined. This can be done by the examiner or recovered for examination by the submitting officer.
3. EnCase does not display images that are attached to e-mail files (i.e. Outlook Express and AOL e-mail files) prior to version 5. If images may be important in a case and an Encase version prior to version 5 is being used, the e-mail files should be recovered to the target drive. These files can be examined by restoring the e-mails to an e-mail account on another computer so that the images attached to the e-mail can be viewed. This examination can be done by the examiner or recovered for examination by the submitting officer. Alternatively, the examiner may use another tool such as Forensic Tool Kit to examine the case for e-mail.
4. Due to the size of modern hard drives, it is not possible to read all of the data recovered in a case. Every effort should be made to search by relevant dates or file types and search by relevant keywords in order to find information pertinent to the case.
5. Microsoft Office 2007 documents are different than previous versions. The following was copied from the Guidance Software website:

"*Microsoft's Office 2007 documents are stored in what is referred to as the Office Open XML File Format. It is a ZIP file of various XML documents describing the entire document.*"
In order to view the contents of these files, they must be mounted like other types of Zip files.
When using version 5 of EnCase, mounting ZIP files will allow you to see the contents of Office 2007 documents.
When using version 6 of EnCase, you must select "Mount Persistant" option inside of the File Mounter EnScript to keep the files mounted after the EnScript completes running. If you do not select this option, the files will unmount as soon as the EnScript finishes running and you will manually have to mount the files by right clicking and viewing file structure.

Title: DVR Analysis Protocol
Version: 1.1 (3/9/2010)

Introduction:
This procedure describes the steps to be taken by all personnel of the North Carolina State Bureau of Investigation Raleigh Crime Laboratory Digital Evidence Unit in performing an analysis of a Digital Video Recorder (DVR) device.

Purpose:
The purpose of this procedure is to establish a methodology for processing video evidence from a Digital Video Recorder (DVR) device.

Equipment:
1. Screwdrivers
2. Permanent marker
3. Forensic Computer or hard drive cloning device
4. Target hard drive
5. Crossover Ethernet cable
6. DVR manufacturer’s owner’s manual and/or software (if provided or downloadable)

Definitions:
Write Blocker – A technology in computer forensics equipment that helps to protect the media from inadvertent alteration or deletion.

Calibration:
The forensic towers used in casework must be verified each day that they are used to ensure that the computer hardware and software are functioning properly. The procedure for this verification process can be found in the Digital Evidence Unit Validation and Calibration Manual.

Limitations:
DVR storage of video and subsequent metadata is often proprietary in format making the data virtually inaccessible.

For some DVRs it is impossible to determine the manufacturer of the device and therefore the analyst will be unable to extract anything from the device without having the device’s owner’s manual provided.

Procedures:
1. Remove the hard drive from the DVR unit.
2. Connect the hard drive to the forensic computer by means of a write-block device (internal write block bay, external write block device, etc.).
3. Attempt to discern the file storage system for the device.

If the hard drive has an easily discernible file system:

4. Export out the video files from the date and time of interest as determined by the submitting agency.
5. Proceed with the processing of the video data in accordance with the Evidence Search Protocol.
6. Return the original drive to the DVR system upon completion of analysis.

If the hard drive does not have an easily discernible file system:

4. Return the original drive to the DVR system.
5. Search for additional means by which to extract the data from the DVR:
    a. If the system has an Ethernet connector, attempt to make an Ethernet connection between the forensic computer and the DVR device by means of the manufacturer's supplied control software and a crossover Ethernet cable.
    b. If the system has a USB connector and a video output, connect a monitor to the DVR and use the manufacturer's means for exporting the data onto the USB device.
    c. If there are no output connectors on the device apart from the video monitor connector, attach a monitor to the system and utilize a camcorder to capture the video data from the attached monitor.

References:

Digital Evidence Unit Validation and Calibration Manual

Notes:

1. The manufacturer's website may need to be consulted in order to download appropriate control software and/or owner's manuals for the DVR device.

Title: Cell Phone Data Extraction Protocol
Version: 1.1 (3/9/2010)

Introduction:

This procedure describes the steps to be taken by all personnel of the North Carolina State Bureau of Investigation in extracting data from various types of cellular phones which may be submitted to the Laboratory.

Purpose:

The purpose of this procedure is to extract data from any cell phones or SIM cards compatible with the Cellebrite.

Equipment:

1. Cellebrite unit with catalog of cellular phone adapter cables
2. Thumb drive
3. Online SAN drive

Definitions:

1. Cellebrite – A universal forensic extraction device for cellular phones.
2. SAN – Networked array of hard drives used as a digital evidence repository.
3. Case Folder – A folder located on the SAN for use in a specific investigation, designated by case number.

Calibration:

There is no calibration required due to the variability of cellular phone models on the market and the lack of a universal standard for performance verification.

Limitations:

1. When a case is submitted to the laboratory that contains a cellular phone, it should be submitted powered off. During processing it is necessary to turn the phone on, therefore great care should be taken to not allow the device to connect to its cellular network. Allowing the phone to receive a signal from the cellular network might result in a change in the data contained on the internal memory of the phone.

Procedures:

1. Wipe the thumb drive prior to data extraction.
2. Follow the instructions in Chapter 3 (Cellular Phones) or Chapter 5 (SIM Cards) of the CeleBrite UFED User Manual for data extraction.
3. Once the data is extracted from the device to the thumb drive, transfer the data from the thumb drive to the case folder located on the SAN storage drive.

References:

1. CelleBrite UFED User Manual
2. Digital Evidence Unit Validation and Calibration Manual

Title: Results Protocol
Version: 1.4 (8/25/2010)

Introduction:
This procedure describes the steps to be taken by all personnel of the North Carolina State Bureau of Investigation in generating case results to be returned to the submitting agency and the prosecutor.

Purpose:
The purpose of this procedure is to provide guidelines for preparing case results to be returned to the submitting agency and the prosecutor that are consistent from case to case.

Equipment:

1. Forensic Tower

Definitions:
None

Calibration:
The forensic towers used in casework must be verified each day that they are used to ensure that the computer hardware and software are functioning properly. The procedure for this verification process can be found in the Digital Evidence Unit Validation and Calibration Manual.

Limitations:
Only CD-R, DVD-R or DVD+R disks may be used to copy recovered files and the forensic image. CD-RW or DVD-RW disks should never be used because the data on the disk may be altered.

Procedures:

1. At the completion of an examination, a new EnCase case file should be created and the evidence files added to this case. This should be done to ensure that the hash values of the evidence files verify completely. If any changes are made to the evidence files during the examination, the hash values will not verify. The verification of the hash values should be documented in the case notes. If the hash values do not verify, this should be reported to the section supervisor immediately.
2. Make a copy of the files which were found to be of evidentiary value onto a CD or DVD. Document the location that the pertinent files were found (logical files, deleted files, slack space, unallocated space). Any CD or DVD that has apparent pornographic images of children copied on it as part of the examination will be labeled to reflect the following:

   "This media may contain contraband and is intended for use by law enforcement in an official criminal investigation.

Dissemination of this material may result in a criminal violation."

3. A copy of the CDs or DVDs containing files recovered in the case should be produced and retained in the Laboratory in order to refresh the memory of an Analyst at a later date. This media is not evidence. If further examination is needed in the case, either the original evidence or the forensic image must be returned to the Laboratory to continue the examination.
4. Other examination documentation will be stored within the laboratory information and reporting system.
5. Make a copy of the forensic image onto a set of CDs or DVDs. These CDs or DVDs will be returned to the submitting agency. If any further analysis needs to be done, the set of CDs or DVDs can be returned to the lab. The target hard drive used to make the forensic image may be wiped and reused in further casework examinations.
6. A laboratory report should be created in laboratory information and reporting system.

References:

1. EnCase Forensic User Manual
2. EnCase Intermediate Analysis and Reporting course guide
3. EnCase Advanced Computer Forensics course guide
4. Forensic Toolkit User Guide
5. Forensic Boot Camp Training Manual
6. Digital Evidence Unit Validation and Calibration Manual

Notes:

1. When a copy of the work product is made on a CD or DVD for retention in the Laboratory and this media contains possible pornographic images of children, the data on this media must be password protected to prevent any unauthorized use of these files.
2. File copy media will be kept in a locked cabinet and a log will be kept of the individuals that place the media in the cabinet.
3. When creating a CD or DVD, the session must be finalized. This will help prevent accidental damage to the CD.

Title: Results Protocol for SAN
Version: 1.3 (8/25/2010)

Introduction:
This procedure describes the steps to be taken by all personnel of the North Carolina State Bureau of Investigation in generating case results to be returned to the submitting agency and the prosecutor.

Purpose:
The purpose of this procedure is to provide guidelines for preparing case results to be returned to the submitting agency and the prosecutor that are consistent from case to case.

Equipment:

1. Forensic Workstation

Definitions:

1. Virtual Machine (VM) – A software emulation of a computer that executes programs like a real machine.

Calibration:
The Virtual Machines used in casework must be verified each day that they are used to ensure that the software is functioning properly. The procedure for this verification process can be found in the Digital Evidence Unit Validation and Calibration Manual.

Limitations:
Only CD-R, DVD-R or DVD+R disks may be used to copy recovered files and the forensic image. CD-RW or DVD-RW disks should never be used because the data on the disk may be altered.

Procedures:

1. At the completion of an examination, a new EnCase case file should be created and the evidence files added to this case. This should be done to ensure that the hash values of the evidence files verify completely. If any changes are made to the evidence files during the examination, the hash values will not verify. The verification of the hash values should be documented in the case notes. If the hash values do not verify, this should be reported to the section supervisor immediately.
2. Make a copy of the files which were found to be of evidentiary value onto a CD or DVD. Document the location that the pertinent files were found (logical files, deleted files, slack space, unallocated space). Any CD or DVD that has apparent pornographic images of children copied on it as part of the examination will be labeled to reflect the following:

"This media may contain contraband and is intended for use by law enforcement in an official criminal investigation. Dissemination of this material may result in a criminal violation."

3. A copy of the CDs or DVDs containing files recovered in the case should be produced and retained in the Laboratory in order to refresh the memory of an Analyst at a later date. This media is not evidence. If further examination is needed in the case, either the original evidence or the forensic image must be returned to the Laboratory to continue the examination.
4. Other examination documentation will be stored within the laboratory information and reporting system.
5. A laboratory report should be created in laboratory information and reporting system.

References:

1. EnCase Forensic User Manual
2. EnCase Intermediate Analysis and Reporting course guide
3. EnCase Advanced Computer Forensics course guide
4. Forensic Toolkit User Guide
5. Forensic Boot Camp Training Manual
6. Digital Evidence Unit Validation and Calibration Manual

Notes:

1. When a copy of the work product is made on a CD or DVD for retention in the Laboratory and this media contains possible pornographic images of children, the data on this media must be password protected to prevent any unauthorized use of these files.
2. File copy media will be kept in a locked cabinet and a log will be kept of the individuals that place the media in the cabinet.
3. When creating a CD or DVD, the session must be finalized. This will help prevent accidental damage to the CD.

Title: Approved Software for Forensic Computer Examinations
Version 1.3 (3/9/2010)

EnCase is a very powerful forensic software package which is used by the NC SBI Crime Laboratory Digital Evidence Unit. The standard protocols used by the NC SBI Digital Evidence unit are written for investigations using EnCase. Other approved forensic software may be used as necessary, at the analyst's discretion. This is a list of the software which is owned by and approved for use in the NC SBI Crime Laboratory Digital Evidence Unit.

Hard Drive Imaging

- EnCase
- SnapBack
- Forensic Tool Kit
- DD/DCFLDD/SDD

Anti-Virus Software

- Trend Micro OfficeScan
- Symantec/Norton Anti-Virus

Deleted File Recovery

- EnCase
- Norton Unerase
- Forensic Tool Kit

Slack and Unallocated Space Recovery

- EnCase
- Norton DiskEdit
- Forensic Tool Kit

Password Recovery

- Ultimate Tool Kit

Optical Media Processing

- CD/DVD Inspector

System Image Creation/Restoration

- Symantec/Norton Ghost
- Image for Windows

Data Carving

- EnCase
- Forensic Tool Kit
- DataLifter

Text String Searches

- EnCase
- Windows ‘Find’ function
- Forensic Tool Kit

Text Viewers

- EnCase
- Quick View Plus
- Microsoft Word
- Wordpad
- Notepad
- Outlook Express
- Adobe Acrobat
- AOL
- Forensic Tool Kit

Graphics Viewers

- EnCase
- Thumbs Plus
- Quick View Plus
- Outlook Express
- AOL
- IrfanView
- XnView
- Forensic Tool Kit

Movie Viewers

- Windows Media Player
- VLC
- QuickTime

Internet/IM History Analysis

- EnCase
- Net Analysis
- Neda-Nama Yahoo Messenger Archive Decoder

Title: Glossary
Version 1.2 (3/9/2010)

BIOS Basic Input Output System. A number of machine code routines that are stored in ROM and available for execution at boot time.

Browser Browser is short for Web Browser. A browser is a computer program that locates and displays pages from the Internet.

Cache A computer’s cache is an area where the computer can temporarily store frequently used data that would otherwise have to be loaded from a slower source. The computer’s cache speeds up the operation of the computer.

CDFS The standard used to describe the file structure on a CD.

Clone The process of performing a sector-by-sector copy operation from the suspect drive to the destination drive. The number of sectors copied is determined by the size of the suspect drive.

Cluster bitmaps Used by NTFS to keep track of free clusters by using a bitmap. This file contains one bit for every cluster on the volume.

Clusters A group of sectors in a logical volume that is used to store files and folders.

Compressed file A file that has been reduced in size via one or more compression techniques.

Compression A method of storing files resulting in great savings in disk storage space. Compressed blocks are checked for validity in the same way as uncompressed one.

Cookie A cookie is a short piece of data that Web servers place on your computer to help identify Web users. Cookies can be used by Web servers to track your Internet browsing habits.

Cylinder The set of tracks on the drive platters that are at the same head position.

Disk An actual piece of hardware that you can hold in your hand. It could be a floppy disk, hard disk, ZIP disk, etc.

DOS Disk Operating System - usually refers to MS-DOS. Operating system which was developed by Microsoft for IBM compatible PCs. Still used today to help control operation on computers, operating beneath the Windows environment.

Drive Geometry The number and position of the bytes, sectors, tracks located on the physical drive.

EXT2 The primary file system used on the Linux operating system.

Fdisk DOS program that provides information about and editing of the partitions on a hard drive.

File entries
Each folder contains a starting cluster and can be expanded or contracted as files are added or removed from the folder. Each file in the folder is represented by a 32 byte entry in the table. The content of a folder “file” is an array of records containing information about the files in the folder. Each entry in the folder can be either a file or another folder. In this way a “tree” structure can be built.

File slack
The space between the logical end and the physical end of a file.

File signature
A few bytes at the beginning of some files (such as graphic or document files) that constitute a unique signature of the file type, regardless of the file extension used.

File allocation table (FAT)
An array of numbers that sits near the beginning of a DOS volume. The length of the numbers is determined by the size of the volume. Each entry in the FAT corresponds directly to one cluster and there is always one FAT entry for every cluster.

Format
DOS command used to prepare a storage medium (hard drive, floppy disk) for reading and writing. Format does not erase data on the disk. It checks for bad sectors and resets the internal address tables (FAT).

Head
A device that rides very close to the surface of the platter and allows information to be read from and written to the platter.

Hyperlink
A hyperlink is a text phrase (which often is a different color than the surrounding text) or a graphic that conceals the address of a Web Site. Clicking on the hyperlink takes you to the Web Site.

Image drive
Same as the target drive.

Internet
The Internet is a worldwide network with more than 100 million computer users that are linked for the exchange of data, news, conversation and commerce. The Internet is a decentralized network that no one person, organization or country controls.

ISDN Line
Integrated Services Digital Network - A phone line that connects two computers to transmit a digital signal between them, as opposed to the analog signal transmitted over normal phone lines. This allows data to be transferred more than twice as fast as with an analog phone line with a 56kbps modem.

Logical file size
The exact size of a file in bytes and is the number represented in the properties for a file. This is different than physical file size.

Logical drive	A drive named by a DOS drive specifier, such as C: or D:. A single physical drive can act as several logical drives, each with its own specifier.
Master boot record	The very first sector of a physical disk (sector zero) is referred to as the MBR It contains machine code that allows the computer to find the partition table and the operating system.
MD5 hash	A 128 bit value that uniquely describes the contents of a file. This is the standard hash code used in forensics.
NTFS	New Technology File System. The file descriptors for every file on an NTFS volume are stored in the Master File Table.
Partition table	Describes the first four partitions, their location on the disk, and which partition is bootable.
PGP	Pretty Good Privacy - Program used to encrypt data on a computer, such as messages on the Internet.
Physical drive	A single disk drive. A single physical drive may be divided into multiple logical drive.
Physical file size	The amount of space that a file occupies on a disk. A file or folder always occupies a whole number of clusters even if it does not completely fill that space.
Plug-Ins	A piece of computer hardware or software that adds a specific feature or service to a larger system.
RAM slack	The space from the end of the file to the end of the containing sector. Before a sector is written to disk, it is stored in a buffer somewhere in RAM.
RAM	Random Access Memory. Volatile read/write memory whose contents are lost when the power is turned off.
ROM	Read Only Memory. Chips that contain a permanent program that is burned on the chip at the factory and maintained when the power is turned off. The information on these chips can be read but not written to.
Root folder	Stored in a known location, this is a tree structure that supports files and folders within folders to an arbitrary depth.
Sector	A group of bytes within a track and is the smallest group of bytes that can be addressed on a drive. The number of bytes in a sector can vary, but is almost always 512.
Spam	Unsolicited “ junk “ e-mail which is sent to persons who did not request it. It is usually commercial e-mail.
Suspect drive	The drive (or drives) that are removed from a subject’s computer or in the possession of a subject that will be imaged for later analysis. This drive is never analyzed; rather is copied so the analysis can be conducted on the forensic image.
System drive	The forensic hard drive used to boot the forensic tower. This is the drive which contains the forensic search tools.

Target drive	The drive that information from the suspect drive is being written to.
Track	Each platter on a disk is divided into thin concentric bands called tracks. Tracks are established when the disk is low level formatted.
Upload	To send or transmit data from your computer to another computer or network.
URL	Universal Resource Locator - An address at which documents or other resources can be found on the Web.
Volume	A mounted partition. There may be only one volume on a floppy or ZIP disk, or there may be several on a hard disk.
World Wide Web	A group of Internet servers that support HTML formatting. The World Wide Web is one part of the Internet.

Title: References
Version 1.1 (11/25/2008)

- AccessData BootCamp Training Manual: AccessData Corp.: Copyright 1987-2006.

- Cybershock, Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Disruption: Winn Schwartau: Thunder’s Mouth press, New York: 2000: ISBN 1-56025-246-4

- Digital Evidence and Computer Crime ; Forensic Science, Computers and the Internet: Eoghan Casey: Academic Press: 2000: ISBN 0-12-162885-X

- DOS for Dummies

- EnCase Certified Examiner Study Guide: Steve Bunting, EnCE, CCFT and William Wei, EnCE, CISSP: Wiley Publishing, Inc, Indianapolis, IN: 2006: ISBN 0-7821-4435-7

- EnCase Version 2, User Manual: Guidance Software, Inc.: Revision 2.0: Copyright 1998 - 2000

- EnCase Version 3.0, User Manual: Richard Keightley : Guidance Software, Inc.: Revision 3.18

- EnCase Forensic Version 5.05 User Manual: Guidance Software, Inc.: Copyright 2006

- EnCase Intermediate Analysis and Reporting: Guidance Software, Inc. : Intermediate Revision 3.05 : Copyright 2002

- EnCase Intermediate Analysis and Reporting: Guidance Software, Inc. : Intermediate Revision 4.01 : Copyright 2002

- EnCase Intermediate Analysis and Reporting: Guidance Software, Inc. : Professional Development & Training Forensic Series : Copyright 2006

- Forensic Toolkit User Guide: AccessData Corp.: Copyright 2003-2004

- High Technology Crime Investigators Handbook, Working in the Global Information Environment: Dr. Gerald L. Kovacich, William C. Boni: Butterworth-Heinemann: 2000: ISBN 0-7506-7086-X

- How Computers Work, Millennium Edition: Ron White: Que, A Division of Macmillan Computer Publishing, USA: 1999: ISBN 0-7897-2112-0

- I-Way Robbery, Crime on the Internet: William C. Boni and Dr. Gerald L. Kovacich: Butterworth-Heinemann: 1999: ISBN 0-7506-7029-0

- Microsoft MS-DOS, User's Guide and Reference Version 5.0: Microsoft Corporation: Document No. SY07661/20885-0391

- Upgrading and Repairing PCs, 12th Edition: Scott Mueller: Que, A Division of Macmillan Computer Publishing, USA: 2000: ISBN 0-7897-2303-4

- Using Microsoft Windows 95, Fourth Edition: Kathy Ivens: Que, A Division of Macmillan Computer Publishing, USA: 1998: ISBN 0-7897-1573-2